الجمهورية الجزائرية الديمقراطية الشعبية
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
وزارة التكوين والتعليم المهنيين
Ministère de la Formation et de l'Enseignement Professionnels

Centre National de l'Enseignement Professionnel à Distance (CNEPD)

المركز الوطني للتعليم المهني عن بعد (م.و.ت.م.ب)

COURS DE MAINTENANCE ET SUIVI DU RESEAUX

SÉRIE N°02

OBJECTIF PÉDAGOGIQUE :

À l'issue de cette série, les stagiaires seront capables de maintenir et d'assurer le suivi du réseau.

PLAN DE LA LEÇON :

I- PROCEDURES DE MAINTENANCE CURATIVE

1- Diagnostic d'un réseau informatique;
2- Outils de diagnostic réseau;
3- Méthode de résolution des problèmes;
4- Processus de consignation des problèmes;
5- La nature des problèmes.

I- PROCEDURES DE MAINTENANCE CURATIVE

Introduction :

La Maintenance est l'ensemble de toutes les actions techniques, administratives et de management durant le cycle de vie d'un bien, destinées à le maintenir ou à le rétablir dans un état dans lequel il peut accomplir la fonction requise. Nous avons vus dans le chapitre précédent les différents types de maintenance parmi eux la maintenance curative.

La maintenance curative consiste à intervenir sur un équipement lorsqu'il présente un problème de dysfonctionnement ou lorsqu'il tombe en panne.
La maintenance curative d'un réseau informatique est une tâche primordiale pour assurer la continuité et la disponibilité des services du réseau.

1- Diagnostic d'un réseau informatique :

1.1- Définition :

Le diagnostic est l'identification de la cause probable de la (ou des) défaillance(s) à l'aide d'un raisonnement logique fondé sur un ensemble d'informations provenant d'une inspection, d'un contrôle ou d'un test.

1.1- Démarche et étapes de diagnostic :

La démarche de localisation de la défaillance et la recherche de sa cause suit plusieurs étapes dans le diagnostic de panne on peut citer **:**

- S'informer sur l'origine de la panne : analyser les informations, les voyants des équipements des utilisateurs, les explications et les faits constatés par l'opérateur, les situer dans le contexte, distinguer les causes réelles ;
- Traçabilité des informations recueillies (demande intervention, ordre de travail) ;
- Analyse de la panne, avec les outils de test ;
- L'utilisation de la documentation constructrice ;

- Les hypothèses du pré diagnostic **:** la formulation des hypothèses et leurs classifications pour vérification ;
- La définition du diagnostic et l'exécution des tests de vérification des hypothèses **:** Analyser la fonction défaillante (en partant de l'action non réalisée et en remontant vers la partie commande) ;
- Préparation de l'intervention, documents liés à l'intervention, schémas, documents constructeur, équipements de protection individuelle, règles de sécurité.

Étape 1 : Identifier ce qui ne va pas. Identifier correctement le problème est un must : si l'on ne sait pas ce qui ne va pas, on a très peu de chances de résoudre le problème. L'interview aide à mener cette étape à bien.

Étape 2 : établir les limites du problème. Savoir jusqu'où s'étend le problème peut conduire à la bonne solution en un minimum de temps. Dans ce cas encore, l'interview est utile. Après plus ample examen, on peut s'apercevoir que ce problème ressemble à un de ceux que l'on a résolus de par le passé. On peut également rechercher les symptômes du problème sur TechNet ou sur sa base de connaissances favorite. On peut également s'apercevoir que ce problème ressemble exactement à un problème documenté dans un article Microsoft. (Bien sûr, le fait de quitter et de relancer Outlook, ou de rebooter le PC client, pour voir si cela résout le problème, est toujours utile.)

Étape 3 : choisir les solutions potentielles. Lister les possibles causes fondamentales des problèmes identifiés aux étapes 1 et 2. Lister également au moins un test de diagnostic (c'est-à -dire un test pour déterminer si cette cause est vraiment responsable) et une solution potentielle (c'est-à -dire une action susceptible de solutionner le problème) pour chaque cause. Affecter des priorités à cette liste en fonction des causes les plus probables. L'objectif de cette étape est d'identifier les solutions potentielles, non de les tester.

Étape 4 : commencer à tester ses solutions. Maintenant que l'on dispose d'une liste des causes possibles avec leurs priorités, il faut commencer à tester les solutions potentielles à ces causes. Mais attention, comme le dit le docteur, " En priorité, ne pas faire de mal ". Avant de démarrer cette étape, il faut être sûr d'avoir de bonnes sauvegardes de la machine sur laquelle on travaille.

Étape 5 : S'assurer que le problème est résolu. Il existe une nuance subtile entre le fait de solutionner un problème et celui de le faire à peu près ou de déguiser ses symptômes. Idéalement, on voudrait solutionner un problème de façon permanente, mais parfois, ce n'est pas possible, ou on ne sait pas comment faire, ou bien encore on ne dispose pas du temps nécessaire pour ce faire, et on est tenté de l'occulter. Le moment est maintenant venu de décider si le problème est non-récurrent, s'il est susceptible de se reproduire, et ce qu'il serait possible de faire pour éviter qu'il se reproduise.

Étape 6 : tenir un journal. Garder une trace qui rappelle ce que semblait être le problème initial, ce qu'il était réellement, et la façon dont on l'a résolu. Les données de ce journal constituent un enregistrement inestimable pour des références futures (voir étape 2), aussi bien que pour toute personne héritant du système de messagerie dont on assure la maintenance. Toutefois, il ne faut pas conserver ces informations sur la machine Exchange Server, sinon il est possible qu'elles deviennent indisponibles quand on en a vraiment besoin. Dans ce journal, il faudrait également inclure une liste de problèmes courants que les utilisateurs peuvent solutionner sans assistance, avec des instructions pour les résoudre. Pour avoir quelques exemples courants, voir l'encadré : " Usual Suspects ".

2- Outils de diagnostic réseau :

Lorsqu'une application réseau ne fonctionne pas comme on l'attend, il est important de pouvoir regarder de plus près ce qui se passe. Même lorsque tout semble fonctionner, il est utile de lancer des diagnostics sur le réseau, pour vérifier qu'il n'y a rien d'anormal. On dispose pour cela de plusieurs outils de diagnostic, qui opèrent à divers niveaux.

Plusieurs outils sont utilisés pour diagnostiquer et détecter les pannes des réseaux informatiques. On peut les résumes dans les points suivants **:**

2.1-Outils de dépannage matériel :

- Rappeler les technologies réseau actuelles (100/1000 Base T, Wifi, CPL, …) ;
- Distinguer HUB et Switch ;
- Comprendre les différents types de VLANs ;
- Identifier les blocages (restrictions) d'un VLAN ;
- Lister les connecteurs de carte réseau ;
- Connaître les connexions RJ-45 et le brochage associé ;
- Identifier un câble réseau (UTP/STP/.FTP, 4/8 fils, droit/croisé) ;
- Comprendre les voyants d'une carte réseau ;
- Situer les fonctions WOL/EPROM/MBA ;
- Analyser le synoptique d'un HUB/Switch ;
- Connaître le brochage des câblages droits et croisés ;
- Comprendre les connexions entre HUBs/Switchs Utiliser une armoire de brassage ;
- Contrôler le brassage d'une prise ;
- Utiliser un testeur de câble ;
- Décrire et analyser un réseau WIFI.

2.2- Outils de dépannage logiciels :

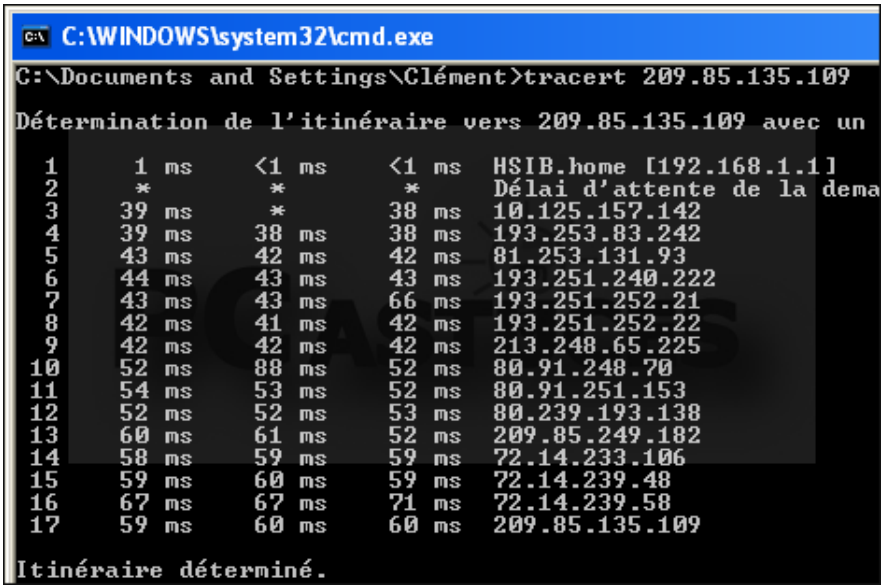
- Comprendre la taxinomie des outils de dépannage courants ;
- Utiliser le diagnostic matériel de Windows (liaison, vitesse, transferts, …) ;
- Comprendre le basculement APIPA sous Windows ;

- Utiliser les commandes WINIPCFG/IPCONFIG (configuration IP) ;
- Décrypter les réponses de la commande PING ;
- Connaître les limites du ping (firewall) ;
- Tester des adresses IP dupliquées (PING et ARP) ;
- Tester des routeurs (PING, TRACERT, PATHPING et ROUTE PRINT) ;
- Utiliser du PING en résolutions de noms (HOSTS/LMHOSTS, WINS et DDNS) ;
- Tester le fonctionnement d'un serveur DNS (ping et NsLookUp) ;
- Identifier les problèmes de cache DNS (IPCONFIG /displaydns et /flushdns) ;
- Tester les services NETBIOS ouverts (NBTSTAT)
- Tester les services IP ouverts (NETSTAT, TCPView, CurrPorts, TELNET, …) ;
- Vérifier la validité du paramétrage réseau de Windows (NETSH) ;
- Utiliser un scanner réseau (Angry IP scanner, SuperScan, WSPING Pro …) ;
- Utiliser un analyseur de trafic (Show Traffic, Wireshark) ;
- Utiliser un analyseur de trame (EtherReal, NetworkActivSniffer,Wireshark … ;
- Identifier une activité réseau anormale (P2P, Virus, Spyware, …) ;
- Identifier les contraintes d'un Firewall (XP SP2) sur le comportement réseau (ping, telnet, Maître Explorateur)

La commande la plus utilisée pour diagnostiquer des problèmes réseau est la commande **ping.** Elle permet de tester la connectivité d'un ordinateur distant, en lui envoyant des paquets de données.

La commande **tracert** quant à elle permet de déterminer l'itinéraire menant vers une destination. Vous pouvez ainsi connaître chaque équipement qui se trouve entre votre ordinateur et la destination que vous indiquez.

La commande **ipconfig** permet d'afficher les valeurs de la configuration actuelle de votre réseau TCP/IP, et d'actualiser au besoin les paramètres DHCP et DNS.

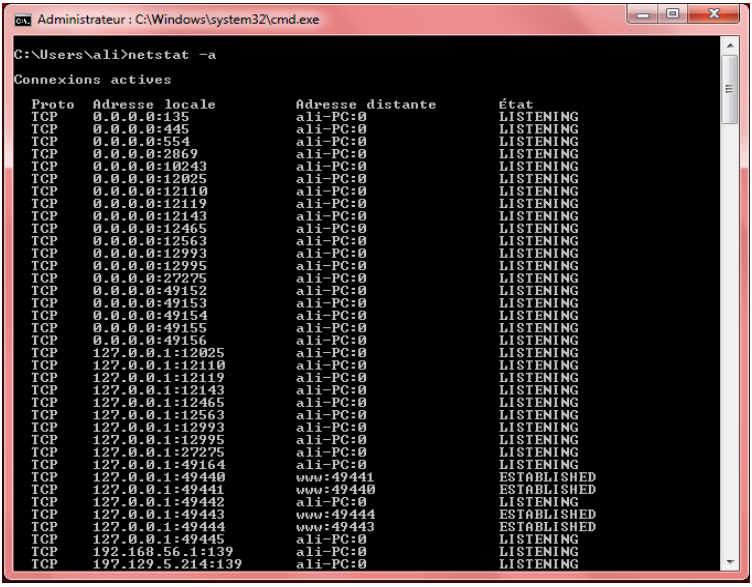


Enfin, en plus de ces commandes, d'autres outils sont inclus dans Windows afin de vous aider à mieux cerner votre environnement réseau et de vous donner des pistes dans la résolution de vos problèmes : arp, netsh, netstat, net, …

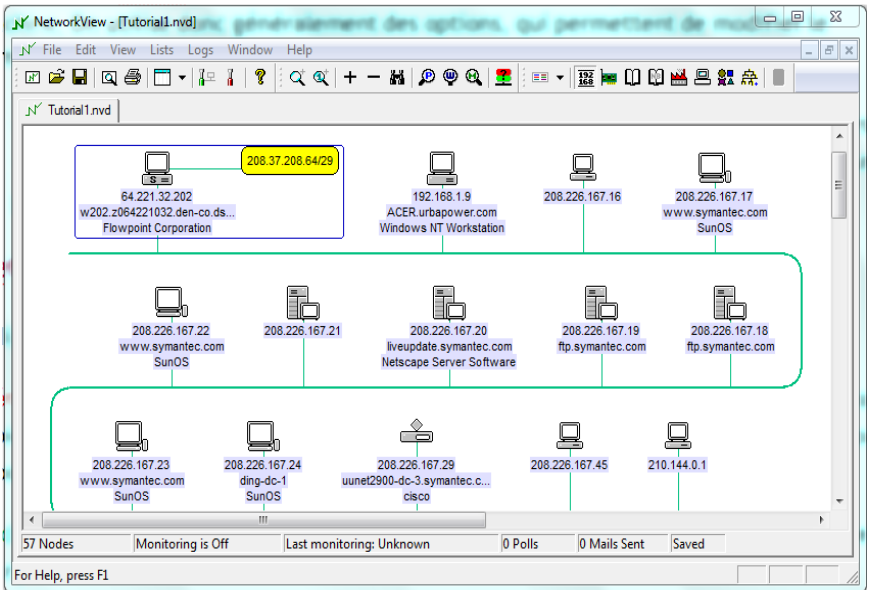
a) Diagnostic local : netstat

La commande **netstat** (du paquet net-tools), qui affiche sur une machine un résumé instantané de son activité réseau. Invoquée sans arguments, cette commande se contente de lister toutes les connexions ouvertes. Or, cette liste est très vite verbeuse et indigeste. En effet, elle inclut aussi les connexions en domaine Unix, qui ne passent pas par le réseau mais sont très nombreuses sur un système standard, car utilisées par un grand nombre de démons.
On utilise donc généralement des options, qui permettent de modifier le comportement de **netstat**. Parmi les options les plus courantes, on trouve **:**

- -t, qui filtre les résultats renvoyés pour que seules les connexions TCP soient listées ;
- -u, qui fonctionne de la même manière mais pour les connexions UDP ; ces deux options ne s'excluent pas mutuellement et la présence des deux aura pour seul effet visible de masquer les connexions du domaine Unix ;
- -a, qui liste également les sockets en écoute (en attente de connexions entrantes) ;
- -n, qui affiche sous forme numérique les adresses IP (sans résolution DNS), les numéros de ports (et non leur alias tel que défini dans /etc/services) et les numéros d'utilisateurs (et non leur nom de connexion) ;
- -p, qui affiche les processus mis en jeu ; cette option n'est réellement utile que lorsque netstat est invoqué par l'utilisateur root, faute de quoi seuls les processus appartenant au même utilisateur seront listés ;
- -c, qui rafraîchit la liste des connexions en continu.



Diagnostic WAN : NetworKView



3- Méthode de résolution des problèmes :

Il est nécessaire de suivre une certaine méthode pour résoudre les problèmes aussi rapidement et efficacement que possible grâce à des processus et procédures communs.

a. La classification :

Il vous permet de déterminer l'étendue et l'impact des problèmes en vue d'établir leur priorité.

b. Test :

Ce processus vise à déterminer la cause probable parmi les causes possibles .après avoir établir la priorité d'un problème et consigné l'incident.

c. Transmission :

On utilise ce processus lorsque le technicien n'arrive pas à résoudre le problème, il le transmettre au support technique de deuxième niveau est un membre de ce service vous posera des questions pour essayer de classifier l'étendue du problème et de définir un niveau priorité.

Rapport :

Lorsque l'incident a été résolu, vous devez documenter sa résolution. Il est important d'enregistrer les modifications apportées à la configuration de votre système informatique. En outre, les problèmes ont tendance à se produire plusieurs fois. S'ils ont été documentés correctement, vous gagnerez du temps la prochaine fois que vous serez amené à résoudre des occurrences similaires du problème.

4- Processus de consignation des problèmes :

Il est important de veiller à ce qu'un processus bien maîtrisé existe au sein de votre organisation pour que les problèmes soient consignés comme il faut.

a. Problème détecté :

Le processus de signalement d'un problème débute lorsque l'utilisateur final détecte un problème de matériel informatique, de système d'exploitation ou d'application
L'utilisateur peut essayer de résoudre le problème lui-même ou contacter le support technique. Si le problème est intermittent, l'utilisateur peut ne pas prendre de mesure immédiate. Si le problème se reproduit, il est possible que l'utilisateur prenne des mesures supplémentaires.

b. Auto-assistance :

Chaque fois que cela est possible, incitez les utilisateurs à trouver eux-mêmes des solutions. Certains problèmes peuvent être résolus très rapidement si l'utilisateur prend le temps de réfléchir à ce qui vient d'arriver.
Proposez toujours une formation adéquate aux utilisateurs finaux. Non seulement ils tireront mieux parti de leurs applications, mais ils seront moins susceptibles de rencontrer des problèmes et seront mieux à mêmes de résoudre nombre de problèmes eux-mêmes, sans contacter le support technique.

c. Contacter le support technique :

Quelles que soient les formations que les utilisateurs finaux auront reçues et quelles que soient vos incitations, ils ne pourront pas résoudre tous les problèmes. Il est important de mettre en place une procédure adéquate pour contacter le support technique afin que les utilisateurs la comprennent bien. Pendant cette phase, consignez les détails du problème.

Pour cela, vous pouvez utiliser une base de données. Vous pouvez ensuite mettre à jour l'enregistrement de base de données à mesure que vous travaillez sur une résolution.
Si vous n'avez pas les compétences nécessaires pour résoudre le problème signalé, assignez le problème à d'autres personnes de votre organisation. Pour les problèmes complexes, vous pouvez réunir une équipe spécialisée. Mettez à jour l'enregistrement dans la base de données de support pour suivre les informations relatives à l'activité que vous, ou d'autres, avez effectuée par rapport au problème signalé.

d. Classification et support initial :

Après que l'utilisateur a contacté le support technique, essayez de classifier le problème et d'en déterminer l'importance et l'urgence. Pour ce faire, vous pouvez poser des questions très spécifiques à l'utilisateur. Il peut s'agir de questions comme celles-ci **:**

- Qui d'autre a le même problème ? Si le problème est répandu, cela indique un problème plus général moins susceptible d'être propre à l'ordinateur de l'utilisateur. En outre, les problèmes qui affectent beaucoup d'utilisateurs sont plus urgents que ce touchant un seul utilisateur.

- Quand avez-vous remarqué le problème pour la première fois ? Il se peut que l'ordinateur n'ait jamais fonctionné correctement. Il est très utile de savoir si l'ordinateur n'a jamais fonctionné correctement, car cela peut indiquer un problème lié au déploiement plutôt qu'à l'utilisation.

- Est-ce que quelque chose a changé à peu près au même moment où vous avez remarqué le problème ? Si l'utilisateur a récemment

installé de nouvelles applications ou mis à jour des pilotes et si le problème est survenu après ces modifications, il est possible que les modifications aient contribué au problème que l'utilisateur signale.

Au cours de cette phase, vous pouvez déterminer une cause probable du problème signalé, mais ne tirez pas de conclusions trop hâtives. Vous risquez autrement de gaspiller beaucoup de temps et de ressources. Votre objectif pendant cette phase est de définir le problème correctement.

e. Transmission :

Lorsqu'un problème doit être transmis à un service de support technique de niveau supérieur ou à des fournisseurs externes, veillez à consigner suffisamment de détails en vue de les transmettre. Il est très utile qu'une procédure de transmission soit clairement définie pour un maximum d'efficacité. La procédure peut stipuler d'inclure les informations suivantes **:**

- Une description précise du problème signalé ;
- Un enregistrement de tous les messages d'erreur associés au problème ;
- Un enregistrement des tentatives de résolution faites par les membres du support technique ainsi que le résultat de chaque tentative ;
- Un enregistrement concernant tous les outils de diagnostic utilisés par les membres du support technique ;
- La durée pouvant s'écouler avant qu'il y ait obligation de transmettre un problème. Vous pouvez considérer de transmettre le problème aux fournisseurs externes dans les cas suivants **:**
- Vous ne pouvez résoudre le problème ; vous ne disposez pas de suffisamment de ressources internes pour résoudre le problème ;
- votre organisation n'a pas les compétences requises pour résoudre le problème ;
- vous avez identifié la cause probable du problème et elle provient d'un composant tiers spécifique ;

- Chaque fois que vous remontez un problème, restez-en toujours le propriétaire et utilisez l'enregistrement de base de données pour suivre la progression vers une résolution ;
- Assurez-vous également que vous fournissez toute l'assistance nécessaire aux autres ;
- Niveaux d'assistance et aux fournisseurs externes.

f. Résolution :

Une fois que vous avez déterminé la cause probable d'un problème et avez développé un plan d'action, vous devez évaluer ce plan. Cette évaluation doit inclure les étapes suivantes **:**

- Faire la liaison avec les spécialistes du support technique impliqués dans l'implémentation du plan ;
- Mener à bien toutes les demandes découlant des procédures de gestion des modifications ;
- Analyser l'impact possible des modifications à l'infrastructure informatique proposées ;
- Détailler les étapes de test du plan proposé ;
- Détailler le plan de restauration des modifications au cas où celles-ci ne produisent pas le résultat escompté.

Après avoir évalué le plan d'action proposé, vous pouvez le mettre en œuvre. Au cas où le plan d'action ne résout pas le problème, envisagez de restaurer les modifications apportées suite à l'évaluation du plan d'action. Vous devez également repenser la phase de classification, car il est possible que le diagnostic et la classification initiaux étaient erronés.

5- La nature des problèmes :

Les problèmes qui affectent les réseaux informatiques peuvent être de **03**natures **:**

a- Problèmes matériel ;
B- Problèmes logiciel ;
C- Problèmes humain**.**

a. Problèmes matériels :

Un problème matériel est un problème qui touche les équipements comme les (PC, câblage, routeurs, switch, etc.) mais il faut distinguer deux genres des pannes :

- Les pannes touchant directement un élément physique d'un système ;
- les pannes touchant la couche logicielle des éléments physiques.

b. Panne logicielle :

C'est une panne qui touche les différents logiciels et applications du réseau informatique comme **:**

- Le Système d'exploitation des hôtes et des serveurs ;
- Les bases de données ;
- Le système d'exploitation des équipements d'interconnexion comme les routeurs et les Switch ;
- Les applications.

c. Problème humains :

Les risques humains sont les plus importants, même s'ils sont le plus souvent ignorés ou minimisés. Ils concernent les utilisateurs mais également les informaticiens eux-mêmes.

- **La maladresse :** comme en toute activité, les humains commettent des erreurs ; il leur arrive donc plus ou moins fréquemment d'exécuter un traitement non souhaité, d'effacer involontairement des données ou des programmes, etc.

- **Le détournement de mot de passe :** un administrateur système ou réseau peut modifier les mots de passe d'administration lui permettant de prendre le contrôle d'un système ou d'un réseau.
- **L'inconscience et l'ignorance :** de nombreux utilisateurs d'outils informatiques sont encore inconscients ou ignorants des risques qu'ils encourent aux systèmes qu'ils utilisent, et introduisent souvent des programmes malveillants sans le savoir.